DEPARTMENT OF THE AIR FORCE
HQ AIR INTELLIGENCE AGENCY

AIA INSTRUCTION 33-111

3 December 1999

Communications and Information

ENTERPRISE INTEROPERABILITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AIA WWW site at: http://pdo.pdc.aia.af.mil/pubs.

OPR: HQ AIA/DOXA (Mr. William Marion)	Certified by: HQ AIA/DOX (Col William Cool)
Supersedes AIAI 33-111, 30 June 1998.	Pages: 12
	Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*, and provides procedures and guidance according to AFI 33-108, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Computer (C4) Systems*, and AFI 33-114, *Software Management*. It establishes Air Intelligence Agency (AIA) guidance and responsibilities to ensure compatibility, interoperability, and integration for new and modified command, control, communications, computer and intelligence (C4I) systems, including Automated Information Systems (AIS). This instruction applies to HQ AIA and its subordinate organizations worldwide; it also applies to AIA-gained Air National Guard and Air Force Reserve units. Refer technical questions to the Architecture and Integration Branch (HQ AIA/DOXA), 102 Hall Blvd, Ste 229, San Antonio TX, 78243-7029. Use AF Form 847, **Recommendation for Change of Publication**, to refer recommended changes and conflicts between this and other publications to HQ AIA/DOXA. Subordinate organizations send one copy of any supplements to HQ AIA/DOXA. See Attachment 1 for references, acronyms, and terms used in this instruction. The use of the name or trademark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed. This instruction also expands the scope to include Defense Information Infrastructure Common Operating Environment (DII COE) related guidance. Removed reference to specific software and replaced with a pointer to the AIA Enterprise Solutions (AES) document which is available on the World Wide Web (WWW) as a living repository for AIA's phased preferred software and hardware baseline.

1. General Information:

1.1. The DII COE. Over the past several decades various Department of Defense (DoD) organizations have developed a number of AIS and C4I systems to enhance the capabilities of the warfighter.

Interoperability between these various systems has only been achieved through brute force means and common functionality has been redeveloped for each individual system. While functional within their given domain, the need to exchange information between these diverse systems drove the DoD, through the Defense Information Systems Agency (DISA), to develop a common operating environment which would provide for the integration of, and interoperability between, diverse mission systems; the DII COE is the result of those efforts. The *Joint Technical Architecture (JTA) Version 1.0* mandated the use of the DII COE for all C4I systems; *JTA Version 2.0* has expanded the applicability of the DII COE to all DoD mission domains. Future versions of the JTA will further enhance its universal applicability to all mission domain standards.

1.2. Diverse Hardware and Software Solutions and Expenditures. AIA must ensure its computer resources are compatible, interoperable, and integrated. AIA will no longer support a multitude of diverse hardware and software solutions with their own distinct training, operational procedures, and troubleshooting skills. The DII COE specifies a baseline of software applications, both Commercial Off-the-Shelf (COTS) and Government Off-the-Shelf (GOTS). The migration to the DII COE requires a great deal of resources, both manpower and money, to achieve; therefore, this instruction implements the AES baseline (for all AIA organizations) and supports the NES baseline (for AIA Signals Intelligence (SIGINT) units) to provide a phased migration to a DII COE-based environment.

2. Roles and Responsibilities:

2.1. The Assistant Director of Operations (HQ AIA/ADO-C) is the AIA Chief Information Officer (CIO). The CIO:

2.1.1. Oversees the agency-wide execution of this instruction.

2.1.2. Bi-annually presents status of this instruction to the AIA Corporate Board. This status update will address interoperability issues, modifications to the AES baseline, and modifications to this instruction.

2.1.3. Has final approval authority on all waivers submitted by AIA organizations, for systems that are under program management control of AIA. Coordinates on all waivers submitted by AIA SIGINT organizations with the Air Force Cryptologic Office (AFCO) and National Security Agency (NSA).

2.1.4. Resolves conflicts in technical architectures promulgated within the Air Force and the intelligence community (IC) for AIA components.

2.1.5. Proposes, coordinates, and advocates resources for AIA-wide standardization initiatives. Advocates AIA site initiatives required to assure site compliance with the AES.

2.1.6. Grants waivers to AES compliance schedules when programmed resources are unavailable.

2.1.7. Provides AIA interface to external organizations on all technical architecture issues.

2.1.8. Reviews and approves and, or disapproves all suggestions for modification to the AES.

2.1.9. Reviews and approves and, or disapproves all suggestions for modification to this instruction.

2.2. HQ AIA/DOXA:

2.2.1. As the CIO Support Staff, assists the AIA CIO in the overall implementation of this instruction.

2.2.2. Staff requests for modification to the AES with the AIA centers, wing, and groups.

2.2.3. Presents coordinated recommendations for AES modification to the AIA CIO.

2.2.4. Presents coordinated recommendations for modifications to this instruction to the AIA CIO.

2.2.5. Maintains this instruction and the related AES and ensures any modifications are in line with all applicable DoD Service and Agency guidance (e.g., guidance from DISA, Defense Intelligence Agency (DIA), NSA, and the USAF).

2.2.6. Coordinates changes to this instruction and the related AES with AIA organizations and the AF Systems Integration Management Office (SIMO) to ensure AIA organization are kept abreast of any modifications that occur.

2.2.7. Reviews and provides recommendations on all waiver requests to the AIA CIO.

2.2.8. Holds an annual AIA Integration Management Review (IMR) at which AIA Centers, Groups and Wing present status of compliance with this instruction.

2.3. 497th Intelligence Group (497 IG):

2.3.1. Serves as AIA interface to DIA on all issues related to the IC migration to the DII COE.

2.3.2. Serves as AIA interface to DISA on all issues related to the IC migration to the DII COE.

2.3.3. Serves as the Department of Defense Intelligence Information Systems (DoDIIS) Executive Agent for Test and Evaluation (DeXA for T&E).

2.4. Det 1, HQ AIA (AFCO):

2.4.1. Serves as AIA interface to NSA for all issues related to national SIGINT mission.

2.4.2. Coordinates with HQ AIA/DOXA on implementation of this instruction and NSAR 10-67.

2.4.3. Validates waiver request and advocates changes to or waivers for SIGINT information technology solutions to NES configuration control board.

2.5. AIA Organizations:

2.5.1. Develop and implement transition plans for the migration of site infrastructures to the DII COE and AES baselines.

2.5.2. Plan and program for site transition to the DII COE and AES baseline

2.5.3. Plan for and execute the segmentation of site-specific systems.

2.5.4. Submit any software or hardware waiver requests to the AIA CIO through HQ AIA/DOXA.

2.5.5. Report status of compliance with this instruction through the annual AIA Site Integration Management Review (SIMR).

3. Standards Guidance:

3.1. DoD Standards Guidance. The JTA is the overarching DoD document which mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. DoD services and agencies may develop standards profiles for a specific mission area that refine the guidance provided within the JTA.

3.2. NSA Standards Guidance (applicable only to AIA SIGINT organizations). NSA Regulation 10-67 and other NSA technical architecture guidance documented in attachment 1 have precedence when discrepancies are noted between the AES and NES baselines. The AIA CIO (through the AFCO) works to resolve these discrepancies to ensure interoperability problems are resolved.

3.3. AIA Standards Guidance. HQ AIA will not develop an AIA specific technical architecture or profile. AIA organizations will comply with the guidance provided by the applicable technical architecture or profile documents listed within attachment 1. AIA organizations should refer to Section 2.2 of the JTA for guidance on standards for the interchange of data and information between applications.

4. AIA Enterprise Solutions:

4.1. Introduction to the AIA Enterprise Solutions (AES):

4.1.1. Overview. The AES documents provide a comprehensive time-phased migration path for all common, non-mission software applications. Additionally, the AES outlines the minimum personal computer and workstation configurations (throughout the remainder of this instruction the term ‘workstation’ will be used to generically refer to end-user or client workstations).

4.1.2. AES Online. The AES is a living document that must evolve with the changing commercial marketplace and evolving DoD guidance. To facilitate the timely revision of the AES, it is maintained as a separate document from this instruction and can be accessed electronically through either the Secret Internet Protocol Router Network (SIPRNET) or Intelink.

4.1.2.1. The AES on SIPRNET. View the AES online through the AIA Products and Services section on SIPRNET. Access the AES link via the publications link from the Products and Services section.

4.1.2.2. The AES on Intelink. The AES can be viewed online through the Products and Services section of AIA Web or HQ AIA Intelink home pages. The AES link can then be accessed via the publications link from the Products and Services section.

4.2. Preferred Software:

4.2.1. Overview. The software listed in the preferred software portion of the AES is subdivided into a number of service areas that mirror the service areas defined in the DII COE architecture. The various service areas are briefly defined below.

4.2.1.1. Kernel, Operating System Services. The applications included in the kernel, operating system services area are the minimal set of software required on every workstation regardless of how the workstation will be used. The kernel components include the operating system and windowing services in addition to six other services to include: basic system administration, basic security administration, an executive manager function (e.g., a desktop Graphical User Interface (GUI) such as Windows NT or the Common Desktop Environment (CDE)), a template for creating privileged operator login accounts, a template for creating non-privileged operator login accounts, and COE tools for segment installation. The operating systems included within the AES are based on DoD, DoDIIS, and USAF target operating systems (TOS) guidance.

4.2.1.2. Infrastructure Services. The applications within the infrastructure services area provide low-level tools for data exchange. These services provide the architectural framework for managing and distributing the flow of data throughout the system. Example services include the Transmission Control Protocol/Internet Protocol (TCP/IP), Distributed Computer Environment (DCE), and the Common Object Request Broker Architecture (CORBA).

4.2.1.3. Common Support Applications. The applications within the common support applications area provide the architectural framework for managing and disseminating information flow throughout a system, and for sharing information among applications. This service area also contains applications for processing and displaying common data formats and for information integration and visualization.

4.2.1.4. Mission Applications. Mission applications sit on top of the COE architecture and access the services provided by the other COE service areas through standard, public Application Program Interfaces (API). Mission applications are GOTS applications and are largely unique to an operational or mission domain. At present, the AES does not directly address mission applications but guidance is provided within this instruction for the migration of AIA-managed mission applications to the DII COE.

4.2.2. Shareware Applications. The restrictions that apply to the use of shareware and, or freeware applications are briefly discussed below.

4.2.2.1. Approving Shareware Applications. The designated approval authority (DAA) must approve all shareware and freeware applications before they are loaded onto AIA-owned platforms. Refer to *Joint DoDIIS Cryptologic SCI Information Systems Security Standards* for guidance.

4.2.2.2. Procuring and Distributing Shareware Applications. Organizations must ensure approved shareware is purchased through official procurement channels and it is distributed in a way that prevents tampering.

4.3. Preferred Workstation Hardware Configuration:

4.3.1. Standardizing Workstation Configurations. As a general requirement, workstations purchased by AIA organizations must meet the minimum hardware requirements of the currently specified TOS and any relevant support and, or mission applications. AIA must standardize, as much as feasible, hardware capabilities to minimize training and maintenance requirements of this hardware.

4.3.2. Preferred Workstation Configuration. The minimum hardware configuration for Windows Intel-based workstations is outlined within the **Preferred Workstation Hardware Configuration** portion of the AES. All hardware purchased for Windows Intel workstations should be on the Microsoft Windows NT Hardware Compatibility List (HCL) or have been tested and found to be compatible with the currently specified version of NT.

5. AES Compliance and Maintenance:

5.1. Reporting Procedures. AIA centers, groups, wing and supported units should report compliance with this instruction through the status briefings presented at the annual AIA SIMR.

5.2. AES Baseline Maintenance. The AES is designed to facilitate an enterprise wide migration to the DII COE product baseline. The DII COE baseline is not static; it evolves in response to trends in the commercial marketplace and various DoD organization's requirements. The AES will evolve in response to changes in the DII COE baseline as well as approved suggestions for modification, addition, and deletion to the AES made by AIA organizations. The following sections provide details on these processes.

5.2.1. Submitting Modifications, Additions and Deletions. AIA organizations may request modifications, additions and, or deletions to the AES through official correspondence from the organization's communications and computers (SC) office or equivalent to HQ AIA/DOXA**.** DOXA will consolidate suggested modifications to the AES and present them to the AIA CIO for approval and, or disapproval. If requested modifications present a major impact across AIA, the AIA CIO presents these issues in his bi-annual presentation to the AIA Corporate Board.

5.2.2. DII COE Software Requirements Process. If warranted, HQ AIA/DOXA consolidates and forwards AIA requirements for software or functionality not included in the existing or projected DII COE baseline to 497 IG/INDS for staffing through the existing DII COE Software Requirements Process.

6. Procuring Hardware and Software:

6.1. Software Licensing and DII COE Asset Distribution:

6.1.1. Enterprise Licenses. Various DoD organizations (DISA, DIA, NSA, USAF, etcetera.) have negotiated (or are negotiating) site licenses for some of the key COTS applications that are included in the AES. Those applications with existing enterprise or site licenses are annotated in the AES. If a site requires an application for which an enterprise license is not available, the site is responsible for planning and programming for the acquisition of the application.

6.1.2. Acquisition of Upgrades. This instruction does not require AIA organizations to accomplish an immediate migration to the AES baseline; rather, as systems or software are upgraded or replaced, AIA organizations should migrate to the applications and specifications referenced within the AES.

6.1.3. DII COE Distribution. All AIA organizations requiring distribution of the segmented DII COE applications should contact the DoDIIS Distribution Facility. Note that delivery of some DII COE COTS segments requires proof of license. Refer to the *DoDIIS Instructions* for further guidance.

6.2. Procuring Workstations:

6.2.1. Contract Vehicle. The standard Air Force contracts such as Blanket Purchase Agreements (BPA), documented in the JTA-AF and the Commercial Information Technology - Product Area Directorate (CIT-PAD) are the first choice for Windows Intel workstation equipment purchases. These BPAs may also be used for the procurement of Windows NT Workstation and Server software as well as the Microsoft Office suite of applications. Where applicable, AIA SIGINT organizations will utilize NSA standard contracts.

6.2.2. Requests for Deviation. Any AIA organization which does not want to use the contract vehicles according to paragraph 6.2.1 for the procurement of workstations, must request a waiver from the AIA CIO through HQ AIA/DOXA.

7. DII COE Segment Certification:

7.1. Overview. One of the key tenets of the DII COE is the concept of segments. Segments, as defined by the *DII COE Integration and Runtime Specification (I&RTS),* are the most basic building blocks from which a COE-based system can be built. They are a collection of related functions as seen from the perspective of the end user, not the developer. Those segments that reside within the COE itself are called *COE-Component Segments* and those segments that reside on top of the COE are *Mission-Application Segments*. The JTA mandates that all command, control, communications, computers, and intelligence (C4I) systems shall use the DII COE. More specifically, it states that all applications of a system that must be integrated into the Defense Information Infrastructure shall be at least DII COE I&RTS Level 5 compliant with a goal of achieving Level 8 compliance. AIA organizations with development responsibility for applications or systems must migrate their systems to the DII COE. The following sections provide some basic information on system segmentation. For more complete information, AIA organizations should consult the appropriate documentation referenced in Attachment 1.

7.2. DoDIIS Migration Systems. Any AIA organization responsible for the development of DoDIIS Migration Systems should adhere to the guidance provided in the *DoDIIS Instructions*. The *DoDIIS Instructions* provide specific guidance on the process for the segmentation and certification of DoDIIS Migration Systems.

7.3. Site-Specific Systems. For the purposes of this instruction, *site-specific systems* are defined as those systems developed by a site which are not distributed for use by any organization external to the site. *Site-unique systems* are those *site-specific systems* that have no requirements or capabilities to interface with systems external to the site. The two basic certification processes available to developers of site-specific systems are explained below.

7.3.1. On-site Certification. The certification of a site-specific, segmented application can be accomplished on-site. The specific details of how this would be accomplished are outside of the scope of this instruction and are left to the discretion of the site. At a minimum the on-site testing must use the *I&RTS* as the basis for determining the level of compliance.

7.3.2. DoDIIS Certification Process. The 497 IG/INDS, as the DeXA for T&E, oversees the DoDIIS Testing and Certification Process which is carried out at the Joint Integration Test Facility (JITF), Rome, New York. Sites can submit their segmented applications for testing at the JITF. The cost of this testing is the responsibility of the site and should be included in the planning process for the migration or transition of the system. Refer to the *DoDIIS Instructions* for additional guidance on this process.

7.4. Segmentation Waiver Request. Site-specific systems, which must interface with other DII COE compliant systems must migrate to the DII COE. If a site feels it is not cost effective to migrate a site-unique system to the DII COE, they must submit a waiver request to the AIA CIO through HQ AIA/DOXA. The waiver should address the rationale for not migrating, impacts on interfacing systems, and should include a cost to benefit analysis.

7.5. Frequently Asked Questions (FAQ). Those AIA organizations with questions regarding the DII COE should consult the AIA DII COE FAQ for additional information regarding the migration to the DII COE. The AIA DII COE FAQ can be found through the Products and Services section of AIA Web on both SIPRNET and Intelink.

JOHN R. BAKER, Maj Gen, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

USAF:

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFI 33-108, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Computer (C4) Systems*

AFI 33-114, *Software Management*

AFI 33-125, *Technical Reference Codes*

CIT-PAD Contract Vehicles. *Http://web1.ssg.gunter.af.mil/CIT-PAD/*

AIA:

AIAI 33-106, *AIA Configuration Management*

Technical Architecture and DII COE:

Department of Defense Joint Technical Architecture, Version 2.0, 26 May 1998.

Secretary of Defense Memorandum, *Implementation of the DoD Joint Technical Architecture*, 22 Aug 96

Air Force Communications Agency, *Joint Technical Architecture - Air Force*, Version 1.3, 15 December 1997

Joint Interoperability and Engineering Organization (JIEO) DISA, *Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS),* Version 3.0, July 1997

Assistant Secretary of Defense for Command, Control, Computers, and Intelligence Memorandum, *Implementation of Defense Information Infrastructure Common Operating Environment Compliance*, 23 May 97

DoDIIS Management Board, *DoDIIS Profile of the DoD Joint Technical Architecture and Defense Information Infrastructure Common Operating Environment*, Version 2.0, 17 September 1998

DIA/DoDIIS:

DIA Memorandum, *GDIP Funded Automated Information Infrastructures and Systems - Statement of Policy,*
5 December 1996

DoDIIS Management Board, *Department of Defense Intelligence Information System (DoDIIS) Instructions*

System Security:

Joint DoDIIS/Cryptologic SCI Information Systems Security Standards, 1 March 1998

NSA:

National Security Agency Enterprise Solutions (NES) Strategy and Implementation Plan, 30 January 1998

NES Baseline (WWW document available from the NSA CIO Intelink homepage)

NSA/CSS Reg 10-67*, Acquisition and Management of Small Computer Assets of NSA/CSS*

NSA Enterprise Solutions (NEW) Strategy and Implementation Plan, 30 January 1998

NSA CIO Memorandum, Implementation of NSA Regulation 10-67, *Acquisition and Management of Small Computer Assets of NSA/CSS (U), 23 March 1998 CIO-038-98*

Unified Cryptologic Architecture Systems Architecture, January 1998

Abbreviations and Acronyms

AES—Air Intelligence Agency Enterprise Solutions

AF—Air Force

AFCO—Air Force Cryptologic Office

AFI—Air Force Instruction

AFPD—Air Force Policy Directive

AIA—Air Intelligence Agency

AIAI—Air Intelligence Agency Instruction

AIS—Automated Information Systems

API—Application Programming Interface

C4—Command, Control, Communications and Computer

C4I—Command, Control, Communications, Computer and Intelligence

CDE—Common Desktop Environment

CIO—Chief Information Officer

CIT-PAD—Commercial Information Technology - Product Area Directorate

CORBA—Common Object Request Broker Architecture

COTS—Commercial Off-the-Shelf

DAA—Designated Approval Authority

DCE—Distributed Computing Environment

DExA—DoDIIS Executive Agent

DExA for T&E—DoDIIS Executive Agent for Test and Evaluation

DIA—Defense Intelligence Agency

DII—Defense Information Infrastructure

DII COE—Defense Information Infrastructure Common Operating Environment

DISA—Defense Information Systems Agency

DoD—Department of Defense

DoDIIS—Department of Defense Intelligence Information Systems

FAQ—Frequently Asked Questions

GOTS—Government Off-the-Shelf

GUI—Graphical User Interface

HCL—Hardware Compatibility List

IC—Intelligence Community

IMR—Integration Management Review

I&RTS—Integration and Runtime Specification

JITF—Joint Integration Test Facility

JTA—Joint Technical Architecture

JTA-AF—Joint Technical Architecture-Air Force

NES—NSA Enterprise Solutions

NSA—National Security Agency

NT—Microsoft Windows NT

RDBMS—Relational Database Management System

RISC—Reduced Instruction Set Computer

SCI—Sensitive Compartmented Information

SHADE—Shared Data Environment

SIMO—Systems Integration Management Office

SIMR—Site Integration Management Review

SIPRNET—Secret Internet Protocol Router Network

TCP/IP—Transmission Control Protocol/Internet Protocol

TOS—Target Operating System

USAF—United States Air Force

WWW—World Wide Web

Terms

Application Programming Interface (API)—1. The interface between the application software and the application platform, across which all services are provided. The API is primarily in support of application portability, but system and application interoperability is also supported by a communications API. 2. A set of formalized software calls and routines that can be referenced by an application program to access underlying network services.

Automated Information System—A combination of information, computer, and telecommunications resources and other information technology and personnel resources that collect, record, process, store, communicate, retrieve, and display information.

Command, Control, Communications and Computer (C4) Systems—Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and across the range of military operations.

Commercial Off-the-Shelf (COTS) Software—Software developed, tested, and sold by commercial companies to the general public. Examples are word processing, graphics, communications, and training software.

Compatibility—Capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference.

Compliance—In the context of the DII COE, an integer value, called the compliance level, which measures (a) the degree to which a segment or system achieves conformance with the rules, standards, and specifications described by the COE, (b) the degree to which the segment or system is suitable for integration with the DII COE reference implementation, and (c) the degree to which the segment or system makes use of COE services.

Government Off-the-Shelf—1. An item of hardware or software that has been produced by or for the government and is available for reuse. 2. Products for which the government owns the data rights, that are authorized to be transferred to other DoD or U.S. Government customers, and that require no unique modifications or maintenance over the life cycle of the product.

Interface—A boundary or point common to two or more similar or dissimilar command and control systems, sub-systems, or other entities against which or at which necessary information flow takes place.

Interoperability—The ability of systems, units or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.

Infrastructure—A term generally applicable to all fixed and permanent installations, fabrications, or facilities for the support and control of military forces.

Segment—In the context of the DII COE, a collection of one or more software and/or data units most conveniently managed as a unit of functionality. Segments are defined from the perspective of an operator, not a developer, and are generally defined to keep related units together so that functionality may be easily included or excluded. They are usually defined as functional pieces (e.g., a word processor) that make sense from a system administrator perspective because segments are the lowest level components that can be installed on, or removed from, a platform.

Segmentation—In the context of the DII COE, the engineering process of decomposing system components into segments and creating the appropriate segment descriptor files.

Shareware—Privately or commercially developed software that is normally distributed free of charge but a fee is generally expected for continued or extended use. Normally, implied or promised support by the author is minimal or nonexistent.